CLAIMS

Sub A1 1. Process for remote and secure payment for goods and/or a service purchased by a buyer (2) from a supplier (7), making use of a mobile radiotelephone (1) used by the said buyer, the said mobile radiotelephone enabling access to a radio communications network (5) managed by a management center (6), a payment server (4) being connected to the said radio communications network (5),

characterized in that the said process includes the following step:

- identification (62) of the said buyer (2) by the said management center (6) and/or the said payment server (4) and/or a control center, the said buyer identification consisting of making sure that the buyer is a subscriber correctly registered on a list of subscribers to the said radio communications network (5).

2. Process according to claim 1, characterized in that the said buyer identification step (62) itself includes the following steps in sequence:

- subscriber identification (62a), enabling the said management center (6) and/or the said payment server (4) and/or the said control center to receive a subscriber identifier (IMSI; 23a; 50) specific to the said buyer, as a user of the said radio communications network;
- subscriber authentication (62b), enabling the said management center (6) and/or the said payment server (4) and/or the said control center to check the said subscriber identifier that was sent to it (them) during the said subscriber identification step (62a).

3. Process according to claim 2, characterized in that the said subscriber authentication step (62b) itself comprises the following steps:

- the said management center and/or the said payment server and/or the said control center supplies a random number (51a) to the said mobile radiotelephone;
- the said mobile radiotelephone generates a subscriber's electronic signature (51b):
  * with an individual authentication algorithm (23b) and/or an individual authentication key (23c) contained in protected areas (23) of the mobile radiotelephone (1), and
  * using the said random number;

- the mobile radiotelephone transmits the said subscriber's electronic signature to the said management center and/or to the said payment server and/or to the said control center;
- the said management center and/or the said payment server and/or the said control center checks the said subscriber's electronic signature.

4. Process according to any one of claims 1 to 3, characterized in that the said process also includes the following step:

- the said management center (6) and/or the said payment server (4) and/or the said control center authenticates (63) the said buyer (2), and possibly a decision to purchase the goods and/or service purchased by the buyer (2).

5. Process according to claim 4, characterized in that the said buyer authentication step, and possibly the purchase decision, itself comprises the following steps:

- the mobile radiotelephone generates a buyer's electronic signature;
- the mobile radiotelephone sends (29a) the said buyer's electronic signature to the said management center and/or the said payment server and/or the said control center;
- the said management center and/or the said payment server (4) and/or the said control center checks (42) the said buyer's electronic signature, the said buyer's electronic signature being kept (43, 44) available for use by the buyer and the supplier.

6. Process according to claim 4, characterized in that the said buyer authentication step, and possibly the purchase decision step, itself comprises the following steps:

- the buyer may input a confidential payment code into the mobile radiotelephone (1), using a keypad (24) associated with the mobile radiotelephone (1);
- the mobile radiotelephone sends a secure transmission of the said confidential payment code to the said management center and/or the said payment server and/or the said control center;
- the said management center and/or the said payment server (4) and/or the said control center checks the said confidential payment code.

7. Process according to claim 5, characterized in that the said buyer authentication step, and possibly the purchase decision, also comprises the following preliminary step:

- the buyer inputs a confidential payment code into the mobile radiotelephone (1) using a keypad (24) associated with the mobile radiotelephone (1).

8. Process according to either of claims 6 and 7 characterized in that the said step in which the said confidential payment code is input, is made using an input algorithm stored in the said mobile radiotelephone.

9. Process according to either of claims 6 and 7 characterized in that the said step in which the said confidential payment code is input, is made using at least one downloaded page in the HDML or an equivalent format provided for this purpose.

10. Process according to any one of claims 5 and 7 to 9, characterized in that the said step in which the buyer's electronic signature is generated is carried out:

- using a payment security algorithm (23d) and/or a payment security key (23e) contained in the protected areas (23) of the mobile radiotelephone (1), and
- starting from data about the transaction and/or data about the buyer.

11. Process according to claim 10, characterized in that at least some of the said data related to the transaction include a variability.

12. Process according to either of claims 10 and 11, the said mobile radiotelephone (1) comprising a terminal (20) cooperating with a subscriber identification module (23), characterized in that the said payment security algorithm and/or the said payment security key is (are) stored in protected areas of the said terminal.

13. Process according to either of claims 10 and 11, the said mobile radiotelephone (1) comprising a terminal (20) cooperating with a subscriber identification module (23), characterized in that the said payment security algorithm (23d) and/or the said payment security key (23e) is (are) stored in protected areas of the said subscriber identification module.

14. Process according to any one of claims 1 to 13, characterized in that it also comprises the following step:

- the mobile radiotelephone (1) is unlocked (61) if a comparison between a confidential identification code (PIN code) contained in protected areas (23) of the mobile radiotelephone (1), and a secret key known to the buyer and input by the buyer into the mobile radiotelephone using a keypad (24), is positive.

15. Process according to any one of claims 3, 10 and 12, the said mobile radiotelephone (1) comprising a terminal (20) cooperating with a subscriber identification module (23), characterized in that at least one some of the said protected areas of the mobile radiotelephone (1) are included in the said subscriber identification module.

16. Process according to any one of claims 1 to 15, characterized in that it also comprises the following step:

- data related to payment for the purchase of goods and/or the service are encrypted (291), exchanged between the mobile radiotelephone and the management center and/or the payment server and/or the control center, to ensure that the purchase is confidential.

17. Process according to any one of claims 1 to 16, characterized in that it also comprises the following step:

- a check (292) of the integrity of data related to payment for the purchase of goods and/or the service exchanged between the mobile radiotelephone and the management center and/or the payment server and/or the control center, so that a defrauder is unable to modify the said data.

18. Process according to any one of claims 1 to 17, characterized in that the said buyer is associated with an electronic wallet (70) comprising:

- a wallet identifier (71) associated with a subscriber identifier (IMSI; 23a; 50) specific to the said buyer, as a user of the said radio communications network;
- means of payment (73, 73a, 73b, 73c);
- information (74) about the said buyer and/or the account(s) of the said buyer;

use of the said means of payment (73), particularly when buying goods and/or a service not being authorized until the buyer has been successfully identified (62), and possibly authenticated (63).

19. Process according to claim 18, characterized in that the said electronic wallet (70) also comprises:

- a confidential payment code (72) known to the said buyer.

20. Process according to either of claims 18 and 19, the said mobile radiotelephone (1) comprising a terminal (20) cooperating with a subscriber identification module (23), characterized in that the said electronic wallet (70) is stored in one of the elements belonging to the group consisting of:

- the said terminal (20),
- the said subscriber identification module (23),
- the said payment server (4),
- the said management center (6),
- the said control center.

21. System for remote payment of goods and/or a service purchased by a buyer (2) from a supplier (7), in a secure manner using a mobile radiotelephone (1) used by the said buyer (2), the said mobile radiotelephone providing access to a radio communications network (5) managed by a management center (6), a payment server (4) being connected to the said radio communications network, characterized in that the said system comprises means of implementing the process according to any one of claims 1 to 20.

22. Mobile radiotelephone (1) used by a buyer for remote payment of goods and/or a service purchased by a buyer (2) from a supplier (7), in a secure manner using a mobile radiotelephone (1) used by the said buyer (2), the said mobile radiotelephone providing access to a radio communications network (5) managed by a management center (6), a payment server (4) being connected to the said radio communications network,
characterized in that the said radiotelephone comprises means of implementing the process according to any one of claims 1 to 20.

FIGURE 5

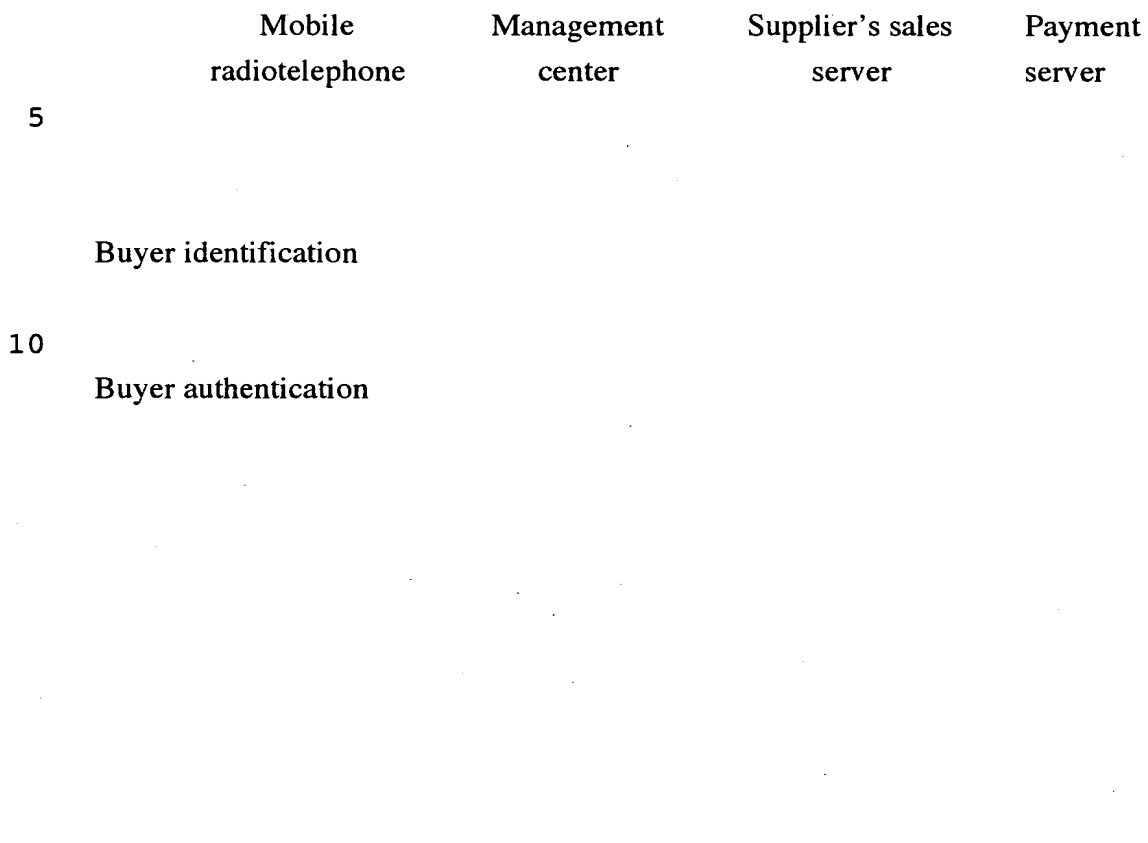

FIGURE 6

Unlock

Buyer identification

Subscriber identification

Subscriber authentication

Buyer authentication